GIUSTIZIA INSIEME

Diritto UE

La Corte di giustizia europea torna ancora sulla data retention

di Federica Resta

23 settembre 2022

La Corte di giustizia europea torna ancora sulla *data retention*

di Federica Resta*

La CGUE riafferma che la conservazione dei dati di traffico, a fini di contrasto dei reati, non può essere generalizzata, preventiva e indifferenziata ma soltanto "mirata" sulla base di criteri specifici. Esclude la possibilità del giudice di limitare gli effetti della declaratoria di invalidità della disciplina interna e prospetta le conseguenze invalidanti dell'acquisizione di elementi probatori sulla base di norme nazionali incompatibili con la disciplina europea. Si ribadisce, inoltre, la distinzione tra gli interessi relativi alla sicurezza nazionale e le esigenze di contrasto dei reati, anche gravi.

1. La sentenza VD

Con le due sentenze in commento, la Corte di giustizia torna a occuparsi della disciplina della *data retention*, consolidando ulteriormente i principi affermati, in particolare, con la pronuncia del 5 aprile 2022, Commissioner of An Garda Síochána e a. (C-140/20, EU:C:2022:258; in questa *Rivista*).

Con tale ultima sentenza, in particolare, la Corte di giustizia aveva chiarito che:

1) l'articolo 15, paragrafo 1, della direttiva 2002/58/CE come modificata dalla direttiva 2009/136/CE non consente, a fini di contrasto della "*criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica*" la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, ma ammette:

– la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione che sia delimitata, sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile;

– la conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione, per un periodo temporalmente limitato allo stretto necessario;

– la conservazione generalizzata e indifferenziata dei dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica, e

– il ricorso a un'ingiunzione rivolta ai fornitori di servizi di comunicazione elettronica, mediante una decisione dell'autorità competente soggetta a un controllo giurisdizionale effettivo, di procedere, per un periodo determinato, alla conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione di cui dispongono tali fornitori di servizi,

sempre che tali misure garantiscano, "*mediante norme chiare e precise, che la conservazione dei dati di cui trattasi sia subordinata al rispetto delle relative condizioni sostanziali e procedurali e che le persone interessate dispongano di garanzie effettive contro il rischio di abusi*";

2) l'articolo 15, paragrafo 1, della citata direttiva 2002/58 è incompatibile con una "*normativa nazionale in forza della quale il trattamento centralizzato delle domande di accesso a dati conservati dai fornitori di servizi di comunicazione elettronica, provenienti dalla polizia nell'ambito della ricerca e del perseguimento di reati gravi, è affidato a un funzionario di polizia, assistito da un'unità istituita all'interno della polizia che gode di una certa autonomia nell'esercizio della sua missione e le cui decisioni possono essere successivamente sottoposte a controllo giurisdizionale*";

3) il diritto dell'Unione non consente la limitazione temporale, da parte del giudice, degli effetti di una declaratoria di invalidità di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, in quanto incompatibile con l'articolo 15, paragrafo 1, della citata direttiva 2002/58, pur essendo l'ammissibilità degli elementi di prova così ottenuti soggetta al principio di autonomia procedurale degli Stati membri, sempreché nel rispetto, in particolare, dei principi di equivalenza e di effettività.

Entrambe le sentenze del 20 settembre scorso (VD e Space Net rese nelle cause, rispettivamente, C-339 e 397/20 e C-793 e 794/19), riaffermano e sviluppano ulteriormente questi principi, ciascuna per un aspetto peculiare.

La prima sentenza (VD, C-339 e 397/20), muove da un rinvio pregiudiziale proposto dalla Corte di Cassazione francese, in un caso riguardante l'acquisizione- nell'ambito di un procedimento penale per i reati di abuso di informazioni privilegiate, abuso secondario di informazioni privilegiate, favoreggiamento, corruzione e riciclaggio- di dati di traffico conservati, per un anno, sulla base della disciplina nazionale rilevante. I quesiti sollevati dalla Corte di cassazione francese concernevano, in particolare:

– l'interpretazione della direttiva e del regolamento sugli «abusi di mercato» (artt. 12, par.2, lett.a) e d), direttiva 2003/6/CE e 23, par. 2, lettere g) e h), regolamento (UE) 596/2014), in combinato disposto con l'art. 15, par.1, della direttiva 2002/58/CE, letta alla luce della Cdfue e la compatibilità, con tale quadro normativo, delle misure legislative nazionali che impongono agli operatori di servizi di comunicazione elettronica, una conservazione generalizzata, preventiva e indiscriminata dei dati relativi al traffico per un anno a decorrere dal giorno della registrazione, a fini di contrasto dei reati di abuso di mercato;

– l'ammissibilità della provvisoria efficacia della normativa interna, laddove ritenuta incompatibile con la disciplina europea, per evitare un'eccessiva incertezza del diritto e consentire l'utilizzazione, a fini probatori, dei dati conservati in forza di tale normativa.

Nelle more della decisione della Corte di giustizia, peraltro, era sopravvenuta la sentenza del 21 aprile 2021 del Conseil d'État (French Data Network e altri: nn. 393099, 394922, 397844, 397851, 424717, 424718), con cui sono state dichiarate illegittime le disposizioni nazionali sulla conservazione generalizzata dei dati di connessione a fini di giustizia, ad eccezione della parte relativa alla conservazione degli indirizzi IP e dei dati relativi all'identità anagrafica degli utenti delle reti di comunicazione elettronica, in linea con la sentenza Cgue 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791).

Con la sentenza VD la Corte di giustizia dichiara oggi incompatibile, con l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8, 11 e 52, paragrafo 1, CDFUE, una normativa nazionale, quale quella considerata, che imponga agli operatori di servizi di comunicazione elettronica -a fini di contrasto dei reati di *market abuse*- - la conservazione generalizzata e indiscriminata dei dati di traffico di tutti gli utenti dei mezzi di comunicazione elettronica, "*senza che sia operata alcuna distinzione al riguardo o che siano previste eccezioni e*

senza che il rapporto richiesto, ai sensi della giurisprudenza menzionata al punto precedente, tra i dati da conservare e l'obiettivo perseguito sia dimostrato" (punto 94). Il richiamo alla giurisprudenza precedente (e, in particolare, alla sentenza del 5 aprile 2022) vale, dunque, a ribadire, sia pur indirettamente, i parametri di ammissibilità della conservazione dei tabulati lì delineati, ovvero criteri soggettivi, geografici o di altra natura (purché oggettivi e non discriminatori) tali da sottendere una relazione funzionale tra le esigenze investigative e il dato da acquisire.

La Corte ribadisce, peraltro, l'inammissibilità di una limitazione, nel tempo, della declaratoria di invalidità della normativa interna che imponga, agli operatori di servizi di comunicazione elettronica, la conservazione generalizzata e indiscriminata dei dati di traffico e ne consenta la comunicazione all'autorità competente, senza previa autorizzazione di un organo giurisdizionale o di un'autorità amministrativa indipendente. Ne risulterebbero, altrimenti, minati il primato e l'esigenza di applicazione uniforme del diritto dell'Unione.

Riprendendo quanto affermato nella sentenza del 2 marzo 2021, H.K. c. Prokuratuur (C 746-18), la Corte precisa, inoltre, che la questione relativa all'ammissibilità degli elementi di prova ottenuti in applicazione delle disposizioni legislative nazionali incompatibili con il diritto dell'Unione è di competenza interna, conformemente al principio di autonomia procedurale degli Stati membri, ferma restando, comunque, l'osservanza dei principi di equivalenza ed effettività.

Relativamente a quest'ultimo principio, la Corte ricorda che esso impone al giudice nazionale di escludere informazioni ed elementi di prova ottenuti mediante la conservazione generalizzata e indiscriminata dei dati di traffico e dei dati relativi all'ubicazione, sulla base di norme incompatibili con il diritto dell'Unione, o anche mediante un accesso dell'autorità competente a tali dati incompatibile con la disciplina europea, laddove la parte nei cui confronti siano utilizzati quegli elementi probatori non possa "*svolgere efficacemente le proprie osservazioni in merito alle informazioni e agli elementi di prova suddetti, riconducibili a una materia estranea alla conoscenza dei giudici e idonei a influire in maniera preponderante sulla valutazione dei fatti*" (punto 106).

2. La sentenza Space Net

Con la sentenza Space Net (C-793/19 e C-794/19), su rinvio pregiudiziale della Corte amministrativa federale tedesca, la Corte conferma l'incompatibilità, con il diritto dell'Unione, di una disciplina interna che preveda, per fini di "*contrasto della criminalità grave e di prevenzione*

delle minacce gravi alla pubblica sicurezza", la conservazione generalizzata e indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione, a titolo preventivo .

In linea con il precedente del 5 aprile 2022, la Corte ribadisce anche la conformità, al diritto dell'Unione, di una disciplina nazionale che, per esigenze di salvaguardia della sicurezza *nazionale,* ammetta l'ingiunzione, nei confronti dei fornitori di servizi di comunicazione elettronica, della conservazione generalizzata e indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione, "*in situazioni nelle quali lo Stato membro interessato affronti una minaccia grave per la sicurezza nazionale che risulti reale e attuale o prevedibile*" (dispositivo.).

Tale ingiunzione – precisa la Corte- deve poter essere oggetto di sindacato, con efficacia vincolante, da parte di un giudice o di un organo amministrativo indipendente diretto ad accertare l'esistenza dei presupposti legittimanti e delle condizioni e delle garanzie necessarie. Essa può, peraltro, essere emessa solo per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile in caso di persistenza dei requisiti.

Parimenti conforme al diritto dell'Unione sarebbe una disciplina interna che, con la previsione di garanzie adeguate a contrastare il rischio di abusi:

a) a fini di salvaguardia della sicurezza *nazionale*, di contrasto dei *"reati gravi e di prevenzione delle minacce gravi alla pubblica sicurezza*", legittimi:

– la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione che sia delimitata, sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile sussistendone i presupposti;

– la conservazione generalizzata e indiscriminata degli indirizzi IP attribuiti all'origine di una connessione, per un periodo temporalmente limitato allo stretto necessario;

– la conservazione generalizzata e indiscriminata dei dati relativi all'identità anagrafica degli utenti di mezzi di comunicazione elettronica;

b) a fini di contrasto dei reati gravi e di salvaguardia della sicurezza *nazionale*, consenta di ingiungere ai fornitori di servizi di comunicazione elettronica, di procedere, per un periodo determinato, alla conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione di cui dispongono.

Anche questa sentenza, dunque, ribadisce e sistematizza le conclusioni della pronuncia del 5 aprile scorso, ivi inclusa la distinzione (rilevante anche in termini di "gerarchia assiologica") tra "

criminalità particolarmente grave" e minacce "*per la sicurezza nazionale*", la cui importanza "*è maggiore rispetto a quella degli altri obiettivi di cui all'articolo 15, paragrafo 1, della direttiva 2002/58*" (punto 72) . In replica a un'eccezione della Commissione europea tesa ad equiparare i due presupposti, la Corte ha ribadito (punti 92-94) che la salvaguardia della sicurezza nazionale corrisponde "*all'interesse primario di tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società, mediante la prevenzione e la repressione delle attività tali da destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un paese, e in particolare da minacciare direttamente la società, la popolazione o lo Stato in quanto tale, quali le attività di terrorismo*". La Corte nota inoltre come, diversamente dalla criminalità, anche particolarmente grave, una minaccia per la sicurezza nazionale debba caratterizzarsi per requisiti di concretezza ed attualità o, quantomeno, prevedibilità, desumibili dalla ricorrenza di "*circostanze sufficientemente concrete da poter giustificare una misura di conservazione generalizzata e indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione, per un periodo limitato*". Tali diversità inducono la Corte a rigettare la tesi della Commissione volta ad equiparare la criminalità particolarmente grave alle minacce per la sicurezza nazionale, così introducendo, ad avviso dei giudici, una categoria intermedia tra la sicurezza nazionale e la pubblica sicurezza, applicando alla seconda i requisiti inerenti alla prima.

Confermato, rispetto alla giurisprudenza precedente, risulta anche l'ambito di ammissibilità della conservazione dei dati di traffico a fini di "giustizia", possibile:

– in misura generalizzata e preventiva per gli indirizzi IP attribuiti all'origine di una connessione (per un periodo temporalmente limitato allo stretto necessario**)** e i dati relativi all'identità anagrafica degli utenti di mezzi di comunicazione elettronica;

– in forma "mirata" rispetto ai dati di traffico ed ubicazione, nel rispetto di criteri selettivi obiettivi e non discriminatori, di ordine soggettivo o geografico (tali cioè da evidenziare un nesso funzionale tra i dati e il reato da accertare), per un periodo temporalmente commisurato secondo stretta necessità;

– nella forma del "quick freeze" dei dati di traffico e di ubicazione.

3. Le implicazioni delle pronunce

Come già il precedente del 5 aprile 2022, anche le sentenze del 20 settembre hanno delle implicazioni rilevanti sulla disciplina vigente della *data retention*, già novellata (per esigenze di conformità alla citata pronuncia Cgue del 2 marzo 2021) dal d.l. 132 del 2021, convertito, con

modificazioni, dalla l. 178 del 2021.

La maggiore distanza tra la disciplina vigente e i principi affermati con la giurisprudenza, ormai consolidata, della Cgue, riguarda il criterio di selettività tale da escludere la massività della misura. La disciplina nazionale riferisce, infatti, il criterio selettivo al solo momento acquisitivo, concependo il criterio della gravità del reato come idoneo a modulare diversamente la profondità cronologica dell'acquisizione processuale, senza tuttavia incidere *ex ante* sulla conservazione. Si tratta di una soluzione certamente coerente con la natura "retrospettiva" di questo mezzo di ricerca della prova, che presuppone una conservazione indistinta in vista di un'acquisizione solo eventuale. Inoltre, essa rispecchia la posizione tenuta dalla Corte costituzionale in relazione alla diversa ingerenza, sulla privacy, della *data retention*, rispetto a quella propria delle intercettazioni, tale da giustificarne in quella prospettiva la differente disciplina (cfr., in particolare, sent. 81 del 1993, che ravvisava nell'acquisizione dei tabulati un'incidenza solo marginale sul diritto alla libertà e segretezza delle comunicazioni di cui all'art. 15 Cost.; posizione che, certo, si inseriva in un contesto sociale assai diverso da quello attuale e si riferiva a ben altre tecnologie).

La posizione della Corte di giustizia è, tuttavia, profondamente diversa e accentua l'impatto significativo della *data retention* sulla riservatezza di tutti i cittadini (nell'ipotesi, appunto, di una conservazione generalizzata, preventiva e indifferenziata) a prescindere da alcuna connessione con possibili reati.

La disciplina interna sembra, dunque, da rivedere, nella parte in cui, pur a fronte di una differenziazione per titolo di reato in fase acquisitiva presuppone, comunque, la conservazione preventiva e generalizzata dei dati di traffico relativi alla generalità indistinta dei cittadini, a fini di "giustizia".

Si dovrà, dunque, ipotizzare una distinzione fondata sulla categoria dei dati, con un regime differenziato e meno rigido (tale dunque da ammettere, anche a fini di giustizia, la conservazione preventiva, sia pur per un tempo proporzionato) per quelli relativi all'identità anagrafica degli utenti e agli indirizzi IP.

Dovranno, poi, essere introdotti parametri di ordine soggettivo, spaziale e se del caso di altra natura (purché, appunto, oggettiva e non discriminatoria) tali da far presumere un nesso funzionale del dato con le esigenze investigative, sulla base dei quali procedere alla conservazione mirata dei dati di traffico e relativi all'ubicazione, da utilizzare a fini di contrasto di reati gravi (categoria da definire sempre secondo il principio di proporzionalità).

Si dovrà, inoltre, disciplinare la conservazione rapida e il relativo accesso con la previsione dei presupposti legittimanti e delle relative garanzie, ivi inclusi, probabilmente, procedimenti di convalida di provvedimenti urgenti, adottati per impedire che il decorso del periodo massimo di memorizzazione a fini commerciali vanifichi elementi probatori.

Rientra, invece, nella sfera di legittimità delineata dalla Corte la conservazione dei tabulati ai sensi dell'art. 4 d.l. 144 del 2005, convertito con modificazioni dalla l. 155 del 2005, in quanto funzionale a fini di sicurezza nazionale. Sul punto resta, tuttavia, da riflettere sull'opportunità di una giurisdizionalizzazione piena anche di questo procedimento acquisitivo, valorizzando la nozione di "giudice" e di indipendenza dell'organo deputato al controllo sulle operazioni conservative cui ricorre la Corte. Tale nozione dovrebbe, infatti, essere coerentemente letta alla luce dell'esigenza di terzietà richiesta, per l'organo titolare del potere autorizzatorio, dalla pronuncia H.K. del 2 marzo 2021 (punto 108, in particolare).

La revisione della disciplina interna della *data retention*, in senso conforme alle indicazioni ormai consolidate ed univoche della Corte di giustizia europea, rappresenta, dunque, un obiettivo importante che il prossimo Parlamento dovrebbe perseguire.

**Dirigente del Garante per la protezione dei dati personali-Le opinioni contenute nel presente contributo sono espresse a titolo esclusivamente personale e non impegnano in alcun modo l'Autorità).*